Compliance Solutions Inc.
Tax Rating Services
Telecom & Sales Tax Services
Corporate Income Tax Services
FCC & State Regulatory Services

407-260-1011 407-260-1033 fax mark@csilongwood.com 242 Rangeline Road, Longwood, FL 32750

February 26, 2019
Via US ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554

RE: Nextiva, Inc.
Form 499 Filer ID: 827231
Annual Customer Proprietary Network Information Compliance Certification;
EB Docket No. 06-36

Dear Ms. Dortch,

Enclosed for filing is the Annual Customer Proprietary Network Information ("CPNI") Compliance Certification; EB Docket No. 06-36, filed on behalf of Nextiva, Inc.

Please do not hesitate to contact me at 407-260-1011 or mark@csilongwood.com if you have any questions or concerns.

Thank you for your assistance in processing this filing.

Sincerely,

Mark G. Lammert, CPA
Tax Preparer for Nextiva, Inc.

cc: Nextiva, Inc.
file: Nextiva, Inc. – PUC - FCC

STATEMENT OF POLICY IN TREATMENT OF CUSTOMER PROPRIETARY NETWORK INFORMATION

1. It is Nextiva, Inc. (hereafter referred to as "Nextiva") policy not to use CPNI for any activity other than permitted by law. Any disclosure of CPNI to other parties (such as affiliates, vendors, and agents) occurs only if it is necessary to conduct a legitimate business activity related to the services already provided by the company to the customer. If the Company is not required by law to disclose the CPNI or if the intended use does not fall within one of the carve outs, the Company will first obtain the customer's consent prior to using CPNI.

2. Nextiva follows industry-standard practices to prevent unauthorized access to CPNI by a person other that the subscriber or Nextiva. However, Nextiva cannot guarantee that these practices will prevent every unauthorized attempt to access, use, or disclose personally identifiable information. Therefore:

   A. If an unauthorized disclosure were to occur, Nextiva shall provide notification of the breach within seven (7) days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI").

   B. Nextiva shall wait an additional seven (7) days from its government notice prior to notifying the affected customers of the breach.

   C. Notwithstanding the provisions in subparagraph B above, Nextiva shall not wait the additional seven (7) days to notify its customers if Nextiva determines there is an immediate risk of irreparable harm to the customers.

   D. Nextiva shall maintain records of discovered breaches for a period of at least two (2) years.

3. All employees will be trained as to when they are, and are not, authorized to use CPNI upon employment with the Company and annually thereafter.

   A. Specifically, Nextiva shall prohibit its personnel from releasing CPNI based upon a customer-initiated telephone call except under the following three (3) circumstances:

      1. When the customer has pre-established a password.

      2. When the information requested by the customer is to be sent to the customer's address of record, or

      3. When Nextiva calls the customer's telephone number of record and discusses the information with the party initially identified by customer when service was initiated.

B. Nextiva may use CPNI for the following purposes:

- To initiate, render, maintain, repair, bill and collect for services;
- To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive , or the unlawful use of, or subscription to, such services;
- To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
- To market additional services to customers that are within the same categories of service to which the customer already subscribes;
- To market services formerly known as adjunct-to-basic services; and
- To market additional services to customers with the receipt of informed consent via the use of opt-in or opt-out, as applicable.

4. Prior to allowing access to Customers' individually identifiable CPNI to Nextiva's joint venturers or independent contractors, Nextiva will require, in order to safeguard that information, their entry into both confidentiality agreements that ensure compliance with this Statement and shall obtain opt-in consent from a customer prior to disclosing the information. In addition, Nextiva requires all outside Dealers and Agents to acknowledge and certify that they may only use CPNI for the purpose for which that information has been provided.

5. Nextiva requires express written authorization from the customer prior to dispensing CPNI to new carriers, except as otherwise required by law.

6. Nextiva does not market, share or otherwise sell CPNI information to any third party.

7. Nextiva maintains a record of its own and its affiliates' sales and marketing campaigns that use Nextiva's customers' CPNI. The record will include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign.

A. Prior commencement of a sales or marketing campaign that utilizes CPNI, Nextiva establishes the status of a customer's CPNI approval. The following sets forth the procedure followed by Nextiva.

- Prior to any solicitation for customer approval, Nextiva will notify customers of their right to restrict the use of, disclosure of, and access to their CPNI.
- Nextiva will use opt-in approval for any instance in which Nextiva must obtain customer approval prior to using, disclosing, or permitting access to CPNI.
- A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.

- Records of approvals are maintained for at least one year.
- Nextiva provides individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.
- The content of Nextiva's CPNI notices comply with FCC rule 64.2008 (c).

8. Nextiva has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This systems allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.

9. Nextiva has a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and will maintain compliance records for at least one year. Specifically, Nextiva's sales personnel will obtain express approval of any proposed outbound marketing request for customer approval of the use of CPNI by The General Counsel of Nextiva.

10. Nextiva notifies customers immediately of any account changes, including address of record, authentication, online account and password related changes.

11. Nextiva may negotiate alternative authentication procedures for services that Nextiva provides to business customers that have a dedicated account representative and a contract that specifically addresses Nextiva's protection of CPNI.

12. Nextiva is prepared to provide written notice within five business days to the FCC of any instance where the opt-in mechanisms do not work properly to such a degree that consumer's inability to opt-in is more than an anomaly.

ANNUAL 47 C.F.R. S: 64.2010 (e) CPNI CERTIFICATION FOR 2019
EB Docket 06-36

Date Filed: January 28, 2019
Name of Company: Nextiva, Inc.
Form 499 Filer ID: 827231
Name of Signatory: David Clark
Title of Signatory: CEO

I, David Clark, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. &64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et. seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. The steps the company has taken to protect CPNI include updating its CPNI practices and procedures and conducting new training designed to ensure compliance with the FCC's modified CPNI rules.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: